Claims

We claim:

1. A method for use in a device associated with a first party for performing a key retrieval operation, the method comprising the steps of:

generating in the first party device a request for the partial assistance of a device associated with a second party in recovering a key from data stored on the first party device, wherein the second party device is remote from the first party device;

transmitting the request from the first party device to the second party device;

receiving results in the first party device generated by the second party device based on the partial assistance provided by the second party device; and

using at least a portion of the received results in the first party device to recover the key for subsequent use as a private key in one or more associated public key cryptographic techniques.

2. The method of claim 1, wherein the first party device is a client device and the second party device is a server.

3. The method of claim 1, wherein the data stored on the first party device has a piece of secret information associated therewith which is included in the request, and further wherein the partial assistance is provided by the second party device when a verification is made by the second party device, based on the piece of secret information, that the first party sent the request.

4. The method of claim 1, wherein the request generated by the first party device comprises cryptographic information included in the data stored on the first party device and previously generated from the key.

5. The method of claim 4, wherein the cryptographic information is generated via an encryption operation which is a function of one or more pieces of secret information associated with the first party, the key, and a public key associated with the second party device.

6. The method of claim 4, wherein the results generated by the second party device comprise results associated with the second party device partially decrypting at least a portion of the cryptographic information in the request.

7. The method of claim 6, wherein the step of using at least a portion of the received results in the first party device further comprises completing the decryption of at least a portion of the cryptographic information to recover the key.

8. The method of claim 1, further comprising the step of at least temporarily storing the recovered key at the first party device.

9. The method of claim 1, wherein the one or more associated public key cryptographic techniques comprise decryption or signature operations.

10. The method of claim 1, wherein no pre-registration process need take place between the first party device and the second party device.

11. A method for use in a device associated with a first party for assisting in the performance of a key retrieval operation, the method comprising the steps of:

receiving a request generating in and transmitted by a second party device for the partial assistance of the first party device in recovering a key from data stored on the second party device, wherein the first party device is remote from the second party device; and

generating results in the first party device based on the partial assistance provided thereby for use in the second party device to recover the key for subsequent use as a private key in one or more associated public key cryptographic techniques.

12. The method of claim 11, wherein the first party device is a server and the second party device is a client device.

13. Apparatus for use in a device associated with a first party for performing a key retrieval operation, the apparatus comprising:

at least one processor operable to: (i) generate in the first party device a request for the partial assistance of a device associated with a second party in recovering a key from data stored on the first party device, wherein the second party device is remote from the first party device; (ii) transmit the request from the first party device to the second party device; (iii) receive results in the first party device generated by the second party device based on the partial assistance provided by the second party device; and (iv) use at least a portion of the received results in the first party device to recover the key for subsequent use as a private key in one or more associated public key cryptographic techniques; and

memory, coupled to the at least one processor, for storing at least a portion of results associated with one or more operations performed by the processor.

14. A method for use in a device associated with a first party for performing a private key operation associated with one or more public key cryptographic techniques, the method comprising the steps of:

generating in the first party device a request for the partial assistance of a device associated with a second party in performing a private key operation using a private key associated with data stored on the first party device, wherein the second party device is remote from the first party device;

transmitting the request from the first party device to the second party device;

receiving results in the first party device generated by the second party device based on the partial assistance provided by the second party device; and

using at least a portion of the received results in the first party device to perform the private key operation.

15. The method of claim 14, further comprising the step of the second party device receiving a request to ignore a subsequent request to perform the partial assistance for a private key operation in order to disable the private key operation.

16. The method of claim 14, wherein the first party device is a client device and the second party device is a server.

17. The method of claim 14, wherein the data stored on the first party device has a piece of secret information associated therewith which is included in the request, and further wherein the partial assistance is provided by the second party device when a verification is made by the second party device, based on the piece of secret information, that the first party sent the request.

18. The method of claim 14, wherein the request to ignore subsequent requests is authenticated by the second party device.

19. The method of claim 14, wherein the step of sharing the performance of the private key operation comprises a function sharing operation.

20. The method of claim 14, wherein the data stored on the first party device was constructed by generating a first share and a second share of a private key associated with the first party device.

21. The method of claim 20, wherein the first share is constructed so that the share can be generated from a piece of secret information associated with the first party and information stored on the first party device.

22. The method of claim 21, wherein the data stored on the first party device comprises an encryption of at least the second share of the private key in accordance with a public key associated with the second party device so as to generate cryptographic information.

23. The method of claim 21, wherein the request generated in the first party device comprises the cryptographic information.

24. The method of claim 23, wherein the step of using at least a portion of the received results in the first party device to perform the private key operation comprises completing a computation of the private key operation at the first party device using results of a computation portion contributed by the second party device.

25. The method of claim 14, wherein the private key operation comprises a decryption operation.

26. The method of claim 25, wherein the decryption operation comprises an ElGamal protocol.

27. The method of claim 14, wherein the private key operation comprises a signature operation.

28. The method of claim 27, wherein the signature operation comprises an RSA protocol.

29. The method of claim 14, wherein no pre-registration process need take place between the first party device and the second party device.

30. A method for use in a device associated with a first party for assisting in performing a private key operation associated with one or more public key cryptographic techniques, the method comprising the steps of:

receiving a request generating in and transmitted by a second party device for the partial assistance of the first party device in performing a private key operation using a private key associated with data stored on the second party device, wherein the first party device is remote from the second party device; and

generating results in the first party device based on the partial assistance provided thereby for use in the second party device to perform the private key operation.

31. The method of claim 30, further comprising, in response to a request, the first party device ignoring a subsequent request to perform partial assistance for a private key operation in order to disable the private key operation.

32. The method of claim 30, wherein the first party device is a server and the second party device is a client device.

33. Apparatus for use in a device associated with a first party for performing a private key operation associated with one or more public key cryptographic techniques, the apparatus comprising:

at least one processor operable to: (i) generate in the first party device a request for the partial assistance of a device associated with a second party in performing a private key operation using a private key associated with data stored on the first party device, wherein the second party device is remote from the first party device; (ii) transmit the request from the first party device to the second party device; (iii) receive results in the first party device generated by the second party device based on the partial assistance provided by the second party device; and (iv) use at least a portion of the received results in the first party device to perform the private key operation; and

memory, coupled to the at least one processor, for storing at least a portion of results associated with one or more operations performed by the processor.

34. The apparatus of claim 33, wherein the second party device receives a request to ignore a subsequent request to perform the partial assistance for a private key operation in order to disable the private key operation.